UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/502,005	07/19/2004	Chin Shyan Ooi	P/2778-50	6804

2352 7590 02/09/2007
OSTROLENK FABER GERB & SOFFEN
1180 AVENUE OF THE AMERICAS
NEW YORK, NY 100368403

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/502,005	OOI ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/2/05; 1/26/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The preliminary amendment of 26 January 2006 has been noted and made of record.

2. Claims 1-20 have been presented for examination.

3. Claims 21 and 22 have been cancelled as per Applicant's request.

Priority

4. Acknowledgment is made of applicant's claim for foreign priority. Receipt is acknowledged of papers submitted, which have been placed of record in the file.

Information Disclosure Statement

5. The information disclosure statements (IDS) submitted on 02 February 2006 and 26 January 2006 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements.

Specification

6. The abstract of the disclosure does not commence on a separate sheet in accordance with 37 CFR 1.52(b)(4). A new abstract of the disclosure is required and must be presented on a separate sheet, apart from any other text.

7. The use of the trademarks ThumbDrive and Windows has been noted on pages 7 and 11, respectively, of this application. They should be capitalized wherever they appear and be accompanied by the generic terminology.

8. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 10-12, and 15-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,618,807 to Wang et al., hereinafter Wang, in view of U.S. Patent No. 7,111,324 to Elteto et al., hereinafter Elteto.

11. As per claim 1, Wang teaches an authentication system to verify a password, the system being arranged for coupling to a host for communication therewith, and comprising:

a first storage unit to store an authentication sequence (Figure 1 [block 30], column 2, lines 61-65, i.e. storing the password in the electronic key);

a read-only memory unit to store an authentication algorithm (Figure 1 [block 26], column 1, lines 42-48, i.e. the crypto program performing password authentication);

a microcontroller (Figure 1 [blocks 18, 22]) coupled to said first storage unit (Figure 1 [block 28]) and said read-only memory unit (Figure 1 [block 20]), wherein said microcontroller is to receive said password and execute said authentication algorithm and wherein said authentication algorithm is to verify said password with said authentication sequence (column 2, lines 38-54, i.e. user inputs password and the crypto program searches for the appropriate password); and

a second storage unit coupled to said microcontroller to store data (Figure 1 [blocks 20, 28], column 1, lines 32-33, i.e. system memory for storing programs and files) and wherein

access to said second storage unit is permitted by said microcontroller only if said password has been verified (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted).

and decrypting data that has previously been encrypted before use thereof in the host (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted).

12. Wang does not disclose a web server and wherein the system is arranged to receive data from the web server, via the host.

13. Elteto teaches a web server (Figures 1, 2, 7, and 8 [block 134]) and wherein the system is arranged to receive data from the web server (column 4, lines 35-62, column 7, lines 37-50, i.e. encrypting files, remotely accessing files).

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to receive encrypted data from a web server, since Elteto states at column 4, lines 2-4 that encrypting files that are transmitted from a remote server implements software protection schemes to prevent copying and unauthorized use of those files, thereby deterring software piracy and hackers from gaining access to said files.

15. Regarding claim 10, Wang teaches an encoder coupled between said microcontroller and said second storage unit, wherein said encoder is to encrypt data that is to be written onto said second storage unit (column 1, lines 35-36, column 2, lines 29-38, i.e. encrypting the program or file).

16. With regards to claim 11, Wang teaches a decoder coupled between said microcontroller and said second storage unit, wherein said decoder is to decrypt data that is to be read from said second storage unit (column 1, lines 35-36, column 2, lines 44-53, i.e. decrypting the program or file).

17. Concerning claim 12, Elteto discloses wherein data stored in said second storage unit is hash-coded (Figures 3 [blocks 302, 304, 306], 4 [block 410], column 8, lines 19-39, column 8, line 53 to column 9, line 8).

18. Regarding claim 15, Wang teaches wherein said first storage unit is located within said read-only memory unit (Figure 1 [block 28], column 2, lines 14-28) and wherein said authentication sequence is hard coded into said first storage unit (Figure 1 [block 30], column 2, lines 14-28).

19. With regards to claim 16, Elteto teaches wherein said second storage area further comprises a public storage area (Figure 3 [block 324]) and a private storage area (Figure 3 [block 326]).

20. Concerning claim 17, Wang and Elteto do not teach wherein said first storage unit is located within said private storage area of said second storage area.

21. It would have been obvious to one of ordinary skill in the art at the time the invention was made have the first storage unit be located within the private storage area of the second

storage unit, since one of ordinary skill in the art would recognize that by having the first storage unit, which contains the encrypted password, part of the private section of the second storage area it would be more difficult for an unauthorized user to gain access to the owner of the electronic key's password.

22. As per claim 18, Wang teaches a method for authenticating a password, comprising:

coupling an authentication system to a host for communication therewith (column 2, lines 14-28, i.e. electronic key can be inserted);

the system receiving said password (column 2, lines 38-54, i.e. user inputs password);

the system providing an authentication sequence (Figure 1 [block 30], column 2, lines 61-65, i.e. storing the password in the electronic key);

the system executing an authentication algorithm (Figure 1 [block 26]) to verify said password with said authentication sequence (column 2, lines 38-54, i.e. user inputs password and the crypto program searches for the appropriate password), wherein said authentication algorithm is stored on a read-only memory unit of the system (Figure 1 [block 26]);

the system permitting access to said data on said storage unit only if said password is verified (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted); and

the system decrypting the data before use in the host (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted).

23. Wang does not disclose the system receiving data from a web server, via the host, in encrypted form, wherein said data is stored in a storage unit of the system.

24. Elteto teaches the system receiving data from a web server, via the host, in encrypted form, wherein said data is stored in a storage unit of the system (column 4, lines 35-62, column 7, lines 37-50, i.e. encrypting files, remotely accessing files).

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made to receive encrypted data from a web server, since Elteto states at column 4, lines 2-4 that encrypting files that are transmitted from a remote server implements software protection schemes to prevent copying and unauthorized use of those files, thereby deterring software piracy and hackers from gaining access to said files.

26. Regarding claim 19, Elteto teaches wherein said password is received from said web server (column 7, lines 37-49, i.e. keys are distributed from a central key to grant access to private documents).

27. With regards to claim 20, Wang discloses wherein said password is entered by a user (column 2, lines 38-54).

28. Claims 2-9 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Elteto as applied to claim 1 above, and further in view of U.S. Patent No. 6,038,320 to Miller, hereinafter Miller.

29. Regarding claim 2, Wang and Elteto do not teach wherein the password is received by said microcontroller from said host.

30. Miller teaches wherein the password is received by said microcontroller from said host (Figure 8 [block 320], column 5, lines 54-64).

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit the password from the host to the microcontroller, since Miller states at column 3, lines 57-67 that by sending the password to an inappropriate security key prevents unauthorized users from accessing the system since the authorized key codes do not match (column 4, lines 47-62), thereby only allowing user's in possession of the security key that contains their password access to the system.

32. With regards to claim 3, Miller teaches a shutdown algorithm to shut down said host and said authentication system after a number of incorrect passwords is received by said microcontroller (Figure 8 [block 300], column 5, lines 1-9, column 5, lines 53-64).

33. With regards to claim 4, Elteto teaches wherein said password is received by said host from said web server (column 7, lines 37-49, i.e. keys are distributed from a central key to grant access to private documents).

34. With regards to claim 5, Wang teaches wherein said authentication algorithm is hard coded on one of a group consisting of a firmware and a hardware in said microcontroller (Figure 1 [block 26], column 2, lines 1-14, column 2, lines 29-64).

35. Concerning claim 6, Wang teaches wherein said second storage unit is a removable storage device (Figure 1 [blocks 18, 28], column 2, lines 14-28).

36. Concerning claim 7, Wang discloses wherein said second storage unit uses flash memory (Figure 1 [blocks 28], column 2, lines 14-28).

37. With regards to claim 8, Wang, Elteto, and Miller all disclose security/electronic keys comprising a USB interface. Elteto illustrates wherein said microcontroller and said read-only memory unit are implemented on a single semiconductor chip in at least figure 2 and column 6, line 60 to column 7, line 9 and column 14, lines 10-33. Figures 2, 4a-c, and 6a-f of U.S. Patent No. 6,848,045 provide even more illustration of the inner workings of the devices disclosed in Wang, Elteto, and Miller, thereby showing that the USB security keys have a microcontroller and memory unit implemented on a single semiconductor chip. This is further supported by figure 1 of Applicant's own patents 6,880,054 and 7,039,759, which clearly shows that USB security keys with a microcontroller and memory unit implemented on a single semiconductor chip was known as early as 2001.

38. Concerning claim 9, Wang, Elteto, and Miller all disclose security/electronic keys comprising a USB interface. Elteto teaches wherein said first storage unit and said read-only memory unit are incorporated into said microcontroller in at least figure 2 and column 6, line 60 to column 7, line 9 and column 14, lines 10-33. Figures 2, 4a-c, and 6a-f of U.S. Patent No. 6,848,045 provide even more illustration of the inner workings of the devices disclosed in Wang,

Elteto, and Miller, thereby showing that the USB security keys have a microcontroller that incorporates a first storage unit and read-only memory. This is further supported by figure 1 of Applicant's own patents 6,880,054 and 7,039,759, which clearly shows that USB security keys have a microcontroller that incorporates a first storage unit and read-only memory was known as early as 2001.

39. Concerning claim 13, Wang and Elteto do not teach wherein said authentication sequence is encrypted.

40. Miller discloses wherein said authentication sequence is encrypted (Figure 4B [block 76], 5 [block 94], 8 [block 340], column 3, lines 47-51, column 4, lines 28-30, column 5, lines 1-9, column 5, lines 53-64).

41. It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the stored password, since one of ordinary skill in the art would realize that, if the security key was ever stolen or came into the possession of an unauthorized user, an encrypted password would provide additional security since any unauthorized users would first have to decrypt the stored password in order to gain access to the user's accounts.

42. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Elteto as applied to claim 12 above, and further in view of U.S. Patent 6,178,508 to Kaufman, hereinafter Kaufman.

43. Concerning claim 14, Wang and Elteto do not teach wherein said authentication sequence is hash-coded.

44. Kaufman discloses wherein said authentication sequence is hash-coded (Abstract, column 2, lines 27-46).

45. It would have been obvious to one of ordinary skill in the art at the time the invention was made to store a hashed password, since Kaufman states at column 2, lines 35-38 that hashing the password prevents the password from being recreated by an unintended party, thereby providing additional security since any unauthorized users that came into possession of the security key would not be able to gain access to the stored password, which prevents the unauthorized user from gaining access to the user's accounts.

Conclusion

46. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

47. The following patents are cited to further show the state of the art with respect to security keys, such as:

United States Patent No. 6,725,382 to Thompson et al., which is cited to show accessing a computer using a portable device.

United States Patent No. 6,848,045 to Long et al., which is cited to show a USB personal security key used for authentication.

United States Patent Application Publication No. 2002/0174287 to Cheng, which is cited to show a co-pending case of the assignee of record.

United States Patent No. 7,036,738 to Vanzini et al., which is cited to show authenticating using a PCMCIA smart card.

United States Patent No. 6,763,399 to Margalit et al., which is cited to show the state of the art with regards to USB keys.

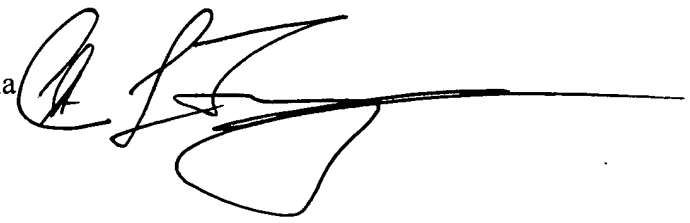
United States Patent Application Publication No. 2004/0025031 to Ooi et al., which is cited to show a co-pending case with at least one common inventor.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

49. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

50. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131



clf